UNIVERSIDAD
DE SANTIAGO
DE CHILE

Departamento de Matemática y Ciencia de la Computación

Laboratorio 1

Algoritmo Key Shedule

Primer Semestre 2018

Criptografía 22633
Licenciatura en Ciencia de la Computación

Gustavo Rojas Torres
gustavo.rojas.t@usach.cl

1 Introducción

El objetivo de este trabajo es análizar e implementar el algoritmo Key Shedule generador de claves para un DES: Data Encryption Standard.

2 Algoritmo implementado

El algoritmo PC-1.

function PC-1
precondition: array[] arreglo de bits, arrayn[] arreglo para las nuevas posiciones en PC-1
postcondition: arreglo PC-1

```
1   begin function
2       cont←0, init←56, i←init
3       for j←0 to 28 do
4           if j=7 or j=15 or j=23
5               array[init]←array[57]
6               i←i+init
7           end if
8           else
9               i←i-8
10          end else
11          cont++
12      end for
13      i←62, v←0
14      for j←28 to 56 do
15          array[j]←array[i]
16          if j=35 or j=43 or j=50
17              if v=2
18                  i←i+23
19              end if
20              else
21                  i←i+(init-2)
22                  v←v+1
23              end else
24          end if
25          else
26              i←i-8
27          end else
28      end for
29  end function
```

La clave de 64-bits primero se reduce a 56 bits ignorando cada bit multiplo de 8. En la permutación PC-1 inicial elimina estos bits. Los bits eliminados no aumentan el espacio clave

El algoritmo PC-2

1 La clave resultante de 56 bits se divide en dos mitades C_0 y D_0.

2 Las dos mitades de 28 bits se giran en una o dos posiciones de bit dependiendo de la ronda i.

3 Las rondas i=1,2,9,16 las dos mitades se giran hacia la izquierda en un bit. El resto de los casos las dos mitades son giradas a la izquierda por dos bits.

El número total de posiciones de rotación es 28.

3 Formulación del experimento

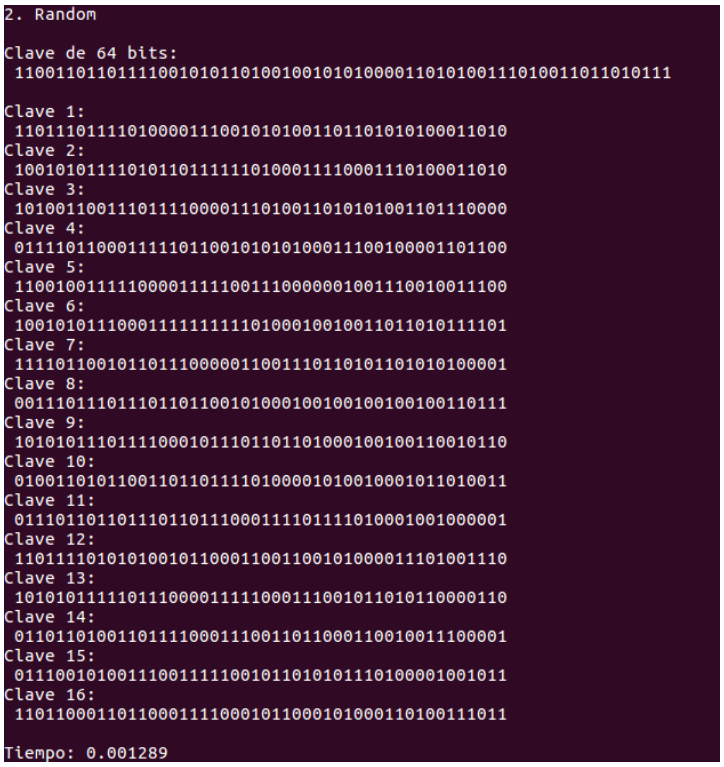
Dado una clave de de 64-bits primero se reduce a 56 bits ignorando cada bit multiplo de 8. En la permutación PC-1 inicial elimina estos bits. Luego esta clave se divide en dos mitades C0 y D0. Las dos mitades de 28 bits de desplazan cíclicamente, es decir, se giran en una o dos posiciones de bit dependiendo de la ronda i según las siguientes reglas:

- Las rondas i=1,2,9,16 las dos mitades son giradas a la izquierda en un bit.
- Las rondas i≠1,2,9,16 las dos mitades son giradas a la izquierda por dos bits.

Las rotaciones solo tienen lugar dentro de la mitad izquierda y derecha. El número total de posiciones de rotación es 4x1+12x2=28. Esto lleva a la propiedad que $C_0 = C_{16}$ y $D_0 = D_{16}$.

Para derivar las claves k_i (de 48 bits cada una) de las 16 rondas del DES, las dos mitades se permutan de nuevo bit a bit utilizando la permutación PC-2. Los 56 bits de entrada de C_i y D_i e ignora 8 bits de C_i y D_i.

4 Curvas de desempeño de resultados



5 Conclusiones

Si bien el Data Encryption Standard (DES) es considerado inseguro para algunos ataques, dado que el conjunto de claves es muy pequeño, es el más popular algoritmo de cifrado de bloques. Aun hoy en día se sigue utilizando en algunas aplicaciones.

6 Forma de Compilación

En la terminal, ubicarse en el directorio donde se encuentra el codigo.c

```
1 gcc lab1.c -o lab1
2 ./lab1
```